REMARKS

This paper is filed in response to the office action mailed on April 1, 2009. In that office action, the drawings, specification and claims 1, 2, 4, 7, 8 and 10 are objected to for informalities; claims 4, 6, 10 and 12 are rejected as being indefinite; and claims 1-3, 5, 7-9, 11 and 13 are rejected as being purportedly obvious in view of prior art. In response, applicants have amended claims 1, 2, 4, 6, 7, 10 and 12. No new matter has been added. In light of the foregoing amendments and following remarks, applicants respectfully request reconsideration and allowance of all pending claims.

Objection to the Drawings

In the outstanding office action, Fig. 1 of the drawings is objected to for failing to label the drawing as Prior Art. In response, applicants have submitted a replacement sheet, filed with this amendment pursuant to 37 CFR §1.121(d), to correct the above-identified labeling error in the drawings of the present application. As the amended drawings are now in an acceptable state, applicants respectfully submit that the objection to the drawings should be withdrawn.

Objection to the Specification

In the office action, the specification is objected to for failing to provide a proper abstract of the disclosure. In response, applicants have amended the specification to correct the error and to add a proper abstract on a new and separate page of the present application. Accordingly, applicants respectfully submit that the objection to the specification should be withdrawn.

Claim Objections

Claims 1, 2, 4, 7, 8 and 10 are also objected to for minor and typographical informalities. Specifically, claim 1 is objected to for lacking a preamble and for not being in proper step format clearly discerning or separating the preamble from the body of the claim. Claim 1 is additionally objected to for lacking indentations for the plurality of steps specified. Claims 1 and 7 are objected to for failing to end with a period. Furthermore, claims 2, 4, 8 and 10 are objected to for failing to spell out the first instance of each abbreviation used therein. In response, applicants have amended claims 1, 2, 4 and 7 to correct each of the aforementioned

errors. Accordingly, applicants respectfully submit that the objections to the claims should be withdrawn.

Claim Rejections – 35 U.S.C. §112

Claims 4, 6, 10 and 12 stand rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctively claim the subject matter which applicant regards as the invention. Particularly, the Examiner finds each limitation of "the group comprising the MD5 function, the SHA-1 function, the SHA-256 function" of claims 4 and 10 as lacking sufficient antecedent basis. The Examiner also finds each limitation of "the combination of a pseudorandom function" of claims 6 and 12 as lacking sufficient antecedent basis. In response, applicants have amended claims 4, 6, 10 and 12 to provide sufficient antecedent basis for each of the aforenoted limitations. Accordingly, applicants respectfully submit that this rejection should be withdrawn.

Claim Rejections – 35 U.S.C. §103

Turning to the prior art rejections, claims 1-3, 5, 7-9, 11 and 13 stand rejected under 35 U.S.C. §103 as being unpatentable over U.S. Patent No. 6,898,753 ("Bonifas") in view of U.S. Patent No. 6,915,473 ("Bolourchi"). However, to support an obviousness rejection, MPEP §2143.03 requires "all words of a claim to be considered" and MPEP §2141.02 requires consideration of the "[claimed] invention and prior art as a whole." Further, the Board of Patent Appeals and Interferences recently confirmed that a proper, post-*KSR* obviousness determination still requires the Office to make "a searching comparison of the claimed invention – including all its limitations – with the teaching of the prior art." *See, In re Wada and Murphy*, Appeal 2007-3733, citing *In re Ochiai*, 71 F.3d 1565, 1572 (Fed. Cir. 1995). Applicants submit that no combination of Bonifas and Bolourchi discloses every limitation of the pending claims, thereby overcoming the aforementioned rejections, as discussed more specifically below.

Claim 1, as well as claims 2-6 dependent thereon, specifies a method of transmitting information which also provides transmission verification. Among other things, claim 1 requires the steps of: (i) transmitting in a frame a useful information message associated with a number p of transmission error verification bits; (ii) obtaining a seal from the useful information message using a sealing function, wherein the seal forms a determined number p1 of

the p transmission error verification bits and p1 is less than p; and (iii) calculating a cyclic redundancy code from the useful information message formed using the p-p1 remaining transmission error verification bits. Claim 7, as well as claims 8-13 dependent thereon, similarly specifies a device for transmitting information with verification of transmission errors. In particular, claim 7 requires at least: (i) means for transmitting in a frame a useful information message associated with a number p of transmission error verification bits; and (ii) means for obtaining a seal from the useful information message using a sealing function, wherein the seal forms a number p1 of said p transmission error verification bits, p1 is less than p, and the p-p1 remaining bits form a cyclic redundancy code calculated from the useful information message.

Bonifas fails to teach or suggest these limitations of the pending claims. The Examiner relies upon the CRC method of Bonifas to assert that Bonifas discloses a useful information message being transmitted in a frame while being associated with a determined number of transmission error verification bits also being transmitted in the frame. Applicants respectfully disagree. Bonifas is solely directed toward use of a cyclic redundancy code (CRC), which consists of transmission error verification bits that are associated with an information message and transmitted in radio frames. The CRC technique and the drawbacks thereof are discussed in much detail in the background of the present application. See paragraphs [0008]-[0016] of the present application, Publication No. 2007/0140259. More specifically, the CRC technique is well known in the art as being a linear function and providing detection at the receiver of unintentional errors which occur during radio transmission over a channel. However, a receiver using the CRC technique cannot detect intentional errors introduced by malicious third parties. For instance, a malicious third party knowing the CRC code can replace a portion of the useful data with corrupted data, and generate CRC bits that are consistent with the corrupted data. The corrupted data is undetectable to a receiver using the CRC technique. As discussed in the present application, it is the mathematical property or linearity of the CRC technique which allows such drawbacks. Among other things, the present application serves to overcome such drawbacks of the prior art by introducing an additional sealing mechanism without reducing the useful bandwidth.

More specifically, and in sharp contrast to Bonifas, the present application teaches a mechanism which authenticates and verifies the integrity of the origin of a communication

signal without requiring additional verification bits to be associated with the transmission data, wherein the term "integrity", as used in the art of data security, relates to the state of the data being unimpaired. It is important to note that the present application is not limited to the addition of bits to the useful data and to the CRC bits, bits which would form a seal obtained from the useful data. In fact, the bits which form the seal are part of the transmission error verification bits, and therefore, provide a dual function seal. As disclosed in the present application, sealing functions not only allow authentication of transmitted data, but further, allow detection of unintentional errors introduced during transmission over a particular channel. More particularly, the present application transmits a dual function seal that is obtained from the useful data and configured to: (i) check the integrity of the transmitted data at the receiver; and (ii) detect any unintentional transmission errors in the data received. Furthermore, the number p, as recited in the pending claims, corresponds to the number of transmission error verification bits that are allocated in a given standard of communication, wherein the bits form a CRC code. Bonifas merely discloses a well known standard use of CRC bits and fails to teach or suggest a dual function seal that is devoted to at least the transmission error verification bits, as required by claims 1 and 7.

Accordingly, Bonifas fails to teach or suggest at least: (i) transmitting in a frame a useful information message associated with a number p of transmission error verification bits; (ii) obtaining a seal from the useful information message using a sealing function, wherein the seal forms a determined number p1 of the p transmission error verification bits and p1 is less than p; and (iii) calculating a cyclic redundancy code from the useful information message formed using the p-p1 remaining transmission error verification bits.

The Examiner admits that Bonifas does not disclose obtaining a seal from the useful information message using a sealing function, wherein the seal forms a determined number p1 of the p transmission error verification bits and p1 is less than p, and calculating a cyclic redundancy code from the useful information message formed using the p-p1 remaining transmission error verification bits, as specified in independent claims 1 and 7. The Examiner thus relies upon Bolourchi to supply the deficiencies of Bonifas. In particular, the Examiner refers to Figs. 4A-B and column 4, lines 1-33 of Bolourchi to assert that Bolourchi discloses numbers M and N transmission error verification bits which form a mask 112 obtained from a

useful message 106 that is transmitted in a determined frame while being associated with a determined number of transmission error verification bits. Applicants respectfully disagree.

Bolourchi discloses a User Equipment Identity (UE ID) that is implicitly included within a CRC without requiring additional overhead signaling. However, the UE ID of Bolourchi is clearly unrelated to a seal as specified in the pending claims. Specifically, the UE ID of Bolourchi is a fixed identification number pertaining to user equipment, and is not a seal that is *obtained from a useful information message using a determined sealing function*, as required by claims 1 and 7. From a structural standpoint, the UE ID of Bolourchi is merely associated with the equipment from which the data originates while the claimed seal is associated with the integrity of the transmitted data and assurance that the data has not been altered during transmission between an emitter and a receiver. Furthermore, Bolourchi is silent as to how the UE ID is retrieved at the receiver when transmission errors are present. When such errors are present, the CRC that is computed on the useful data that is received would be inherently different from the CRC that is included in the received data. According to column 6, lines 58-65 of Bolourchi, Bolourchi does not allow retrieval of the corrected UE ID in such circumstances.

Accordingly, Bolourchi fails to supply all of the aforenoted deficiencies of Bonifas. Specifically, Bolourchi fails to teach or suggest at least: (i) transmitting in a frame a useful information message associated with a number p of transmission error verification bits; (ii) obtaining a seal from the useful information message using a sealing function, wherein the seal forms a determined number p1 of the p transmission error verification bits and p1 is less than p; and (iii) calculating a cyclic redundancy code from the useful information message formed using the p-p1 remaining transmission error verification bits, as required by claims 1 and 7.

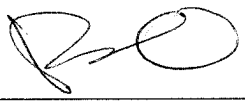
As the purported combination of Bonifas and Bolourchi fails to teach or suggest every limitation of the pending claims, the obviousness rejection of claims 1-3, 5, 7-9, 11 and 13 based upon Bonifas and Bolourchi must also fail and must be withdrawn.

CONCLUSION

In light of the foregoing, applicants respectfully submit that each of the currently pending claims, i.e. claims 1-13, are in a condition for allowance and respectfully solicit the same. If a telephone call would expedite prosecution of the subject application, the Examiner is invited to call the undersigned agent. The undersigned verifies that he is authorized to act on behalf of the assignee of the present application.

Dated: August 10, 2009

Respectfully submitted,



By_____
Robin S. O
Registration No.: 60,043
MILLER, MATTHIAS & HULL
One North Franklin Street
Suite 2350
Chicago, Illinois 60606
(312) 235-4763
Agent for Applicant